FIVE SQUARES IN ARITHMETIC PROGRESSION OVER QUADRATIC FIELDS

ENRIQUE GONZÁLEZ-JIMÉNEZ AND XAVIER XARLES

Abstract. We give several criteria to show over which quadratic number fields $\mathbb{Q}(\sqrt{D})$ there should exists a non-constant arithmetic progressions of five squares. This is done by translating the problem to determining when some genus five curves C_D defined over $\mathbb{Q}$ have rational points, and then using a Mordell-Weil sieve argument among others. Using a elliptic Chabauty-like method, we prove that the only non-constant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{409})$, up to equivalence, is $7^2, 13^2, 17^2, 409, 23^2$. Furthermore, we give an algorithm that allow to construct all the non-constant arithmetic progressions of five squares over all quadratic fields. Finally, we state several problems and conjectures related to this problem.

1. Introduction

A well known result by Fermat, proved by Euler in 1780, says that there does not exists four squares over $\mathbb{Q}$ in arithmetic progression. Recently, the second author showed that over a quadratic field there are not six squares in arithmetic progression (see [13]). As a by-product of his proof one gets that there does exists five squares in arithmetic progression over quadratic fields, but all obtained from arithmetic progressions defined over $\mathbb{Q}$. The aim of this paper is to study over which quadratic fields there are such sequences of five squares, in a similar way that the first author and J. Steuding studied the four squares sequences in [9].

There is a big difference, however, between the four squares problem and the five squares problem: in case a field contain four squares in arithmetic progression, then it probably contains infinitely many (non equivalent modulo squares). But any number field can contain only a finite number of five squares in arithmetic progression: the reason is that the moduli space parametrizing that objects is a curve of genus 5 (see section 3), hence can contain only a finite number of points over a fixed number field by Faltings' Theorem.

On the other hand, one can easily show (remark 34, section 8), that there exists infinitely many arithmetic progressions such that their first five terms are squares over a quadratic field. The conclusion is that there are infinitely many quadratic fields having five squares in arithmetic progression.

In this paper we will try to convince the reader that, even there are infinitely many such fields, there are few of them. For example, we will show that there are only two

Date: October 22, 2009.

2000 *Mathematics Subject Classification.* Primary: 11G30, 11B25,11D45; Secondary: 14H25.

Key words and phrases. Arithmetic progressions, squares, quadratic fields, Elliptic Chabauty, Mordell-Weil Sieve.

The first author was partially supported by the grant MTM2006–10548 and CCG08–UAM/ESP–3906. The second author was partially supported by the grant MTM2006–11391.

fields of the form $\mathbb{Q}(\sqrt{D})$, for D a squarefree integer with $D < 10^{13}$ having five squares in arithmetic progression: the ones with $D = 409$ and $D = 4688329$ (see Corollary 33). To obtain this result we will develop a new method, related to the so-called Mordell-Weil sieve, to show that certain curves have no rational points.

The outline of the paper is as follows. In section 2 we give another proof of a result in [13] that is essential for our paper: any arithmetic progression such that their first five terms are squares over a quadratic field is defined over $\mathbb{Q}$. Using this result we will show in section 3 that a field $\mathbb{Q}(\sqrt{D})$ contains five different squares in arithmetic progression if and only if some curve C_D defined over $\mathbb{Q}$ has $\mathbb{Q}$-rational points. After that we study a little bit the geometry of these curves C_D. In the next sections we give several criteria in order to show when $C_D(\mathbb{Q})$ is empty: when it has no points at $\mathbb{R}$ or at $\mathbb{Q}_p$ in section 4, when has an elliptic quotient of rank 0 in section 5, and when it does not pass some kind of Mordell-Weil sieve at section 6. Section 7 is devoted to compute all the rational points for C_{409}. This is done by a modification of the elliptic Chabauty method, developed by Bruin in [3]. We obtain that there are only 16 rational points coming all from the arithmetic progression $7^2, 13^2, 17^2, 409, 23^2$. Finally, in the last section, we give some tables related to the computations, some values of D where we do have rational points in C_D, and we state several problems and conjectures.

We want to thank Gonzalo Tornaria for helping us in some computations concerning the Corollary 33.

2. The 5 squares condition

Recall that n elements of a progression $a_0, \dots, a_n$ on a field K are in arithmetic progression if there exists a and $r \in K$ such that $a_i = a + i \cdot r$ for any $i = 0, \dots, n$. This is equivalent, of course, of having $a_i - a_{i-1} = r$ fixed for any $i = 1, \dots, n$. Observe that, in order to study squares in arithmetic progression, we can and will identify the arithmetic progressions $\{a_i\}$ and $\{a_i'\}$ such that there exists a $c \in K^*$ with $a_i' = c^2 a_i$ for any i. Hence, if $a_0 \neq 0$, we can divide all a_i by a_0, and the corresponding common difference is then $q = a_1/a_0 - 1$ and it is uniquely determined.

Let $K/\mathbb{Q}$ be a quadratic extension. The aim of this section is to show that any non-constant arithmetic progression whose first five terms are squares over K is defined over $\mathbb{Q}$ modulo the identification above. Another proof of this result can be found in [13].

First, we consider the case of four squares in arithmetic progression over K.

Proposition 1. *Let $K/\mathbb{Q}$ be a quadratic extension, and let $x_i \in K$ for $i = 0, \dots, 3$ be four elements, not all zero, such that $x_i^2 - x_{i-1}^2 = x_j^2 - x_{j-1}^2 \in K$ for all $i, j = 1, 2, 3$. Then $x_0 \neq 0$; and if we denote by $q := (x_1/x_0)^2 - 1$, then $q = 0$ or*

$$\frac{(3q+2)^2}{q^2} \in \mathbb{Q}.$$

Proof. Observe first that the conditions are equivalent to the x_i verify the equations

$$x_0^2 - 2x_1^2 + x_2^2 = 0\ ,\ x_1^2 - 2x_2^2 + x_3^2 = 0,$$

which determine a curve C in $\mathbb{P}^3$. Observe also that q is invariant after multiplying all the x_i by a constant, so we can work with the corresponding point $[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3$. Using the equations above, one shows easily that x_0 can not be zero.

Before continuing, let's explain the strategy of the proof. Due to there are not four squares in arithmetic progression over $\mathbb{Q}$, the genus one curve C satisfies $C(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1]\}$. Suppose we have a non-constant map $\psi : C \to E'$ defined over $\mathbb{Q}$, where E' is an elliptic curve defined over $\mathbb{Q}$, such that $\psi(P) = 0$ for all $P \in C(\mathbb{Q})$. Given any point $P \in C(K)$, denote by $Q := \psi(P) \in E(K)$. Now, consider $\sigma(P) \in C(K)$, where σ denotes the only automorphism of order two of K, so $Gal(K/\mathbb{Q}) = \{\sigma, id\}$. Then $\psi(P) \oplus \psi(\sigma(P))$ must be 0, so $\psi(\sigma(P)) = \sigma(\psi(P)) = \ominus P$. Hence $x(\psi(P)) \in \mathbb{Q}$. Now, the only thing we need to show is that $x(\psi(P)) = \frac{(3q+2)^2}{q^2}$ and we are done.

First observe that, we can suppose that $x_0^2 = 1$, and then $x_i^2 = 1 + iq$ for $i = 1, 2, 3$. Multiplying these three equations we get that

$$(x_1 x_2 x_3)^2 = (q + 1)(2q + 1)(3q + 1).$$

So, changing q by $(x - 2)/6$, and $x_1 x_2 x_3$ by $y/6$, we get the elliptic curve E given by the equation

$$y^2 = x^3 + 5x^2 + 4x,$$

with a map given by $f(1, x_1, x_2, x_3) = (6(x_1 - 1), 6x_1 x_2 x_3)$. This map is in fact an unramified degree four covering, corresponding to one of the descendents in the standard 2-descent. It sends the 8 trivial points to the points $(2, \pm 6)$, which are torsion and of order 4. We need a map that sends some trivial point to the zero, so we just take $\tau(P) := P \oplus (2, -6)$. The map $\tau : E \to E$ (not a morphism of elliptic curves) has equations

$$\tau(x, y) = \left(\frac{2(x^2 + 14x + 6y + 4)}{(x - 2)^2}, -\frac{6(6xy + x^3 + 16x^2 + 32x + 12y + 8)}{(x - 2)^3} \right).$$

The trivial points then go to the 0 point and the point $(0, 0)$.

Now consider the standard 2-isogeny $\mu : E \to E'$, where E' is given by the equation $y^2 = x^3 - 10x^2 + 9x$, given by

$$\mu(x, y) = \left(\frac{y^2}{x^2}, \frac{y(4 - x^2)}{x^2} \right)$$

(see for example [11], example III.4.5.).

The composition $\mu \circ \tau \circ f$ is exactly the map ψ we wanted. By applying the formulae above we get that the x-coordinate of $\mu(\tau(f(1, x_1, x_2, x_3)))$ is exactly equal to $\frac{(3q+2)^2}{q^2}$. $\square$

We apply this proposition to get the result on five squares in arithmetic progression.

Corollary 2. *Let $K/\mathbb{Q}$ be a quadratic extension, and let $x_i \in K$ for $i = 0, \dots, 4$ be five elements, not all zero, such that $x_i^2 - x_{i-1}^2 = x_j^2 - x_{j-1}^2 \in K$ for all $i, j = 1, 2, 3, 4$. Then $x_0 \neq 0$, and if we denote by $q := (x_1/x_0)^2 - 1$, then $q \in \mathbb{Q}$.*

Proof. Suppose $q \neq 0$. By the proposition we have that $t_q := (3q+2)^2/q^2 \in \mathbb{Q}$ and that, if we denote by $q' := (x_2/x_1)^2 - 1$, the same is true for q'. But $q' = q/(q+1)$, so the condition for q' is equivalent to $t'_q := (5q+2)^2/q^2 \in \mathbb{Q}$. But $t'_q - t_q = 16 - 8/q$, so $q \in \mathbb{Q}$. $\square$

3. A diophantine problem over $\mathbb{Q}$

Let D be a squarefree integer. In the above section we have showed that any arithmetic progression of 5 squares over $\mathbb{Q}(\sqrt{D})$ is in fact defined over $\mathbb{Q}$. That is, if we have $x_0,\dots,x_4\in\mathbb{Q}(\sqrt{D})$ such that $x_i^2-x_{i-1}^2=x_j^2-x_{j-1}^2$ for all $i,j=1,2,3,4$, then, after changing the progression by an equivalent progression, we have that $x_i^2=d_iX_i^2$ where $d_i=1$ or D and $X_i\in\mathbb{Q}$. We say that such arithmetic progression $x_0^2,\dots,x_4^2$ is of type $I:=\{i\,:\,d_i=D\}\subset\{0,\cdots,4\}$.

Observe that two such arithmetic progressions $x_0^2,\dots,x_4^2$ and $y_0^2,\dots,y_4^2$ over $\mathbb{Q}(\sqrt{D})$ are equivalent if there exists $\alpha\in\mathbb{Q}^2$ or $\alpha\in D\,\mathbb{Q}^2$ such that $y_i^2=\alpha x_i^2$, $i=0,\dots,4$. Moreover, we will identify the sequences such that $y_{4-i}^2=x_i^2$ for all $i=0,\dots,4$. Up to these equivalences, there are only few types of non-constant arithmetic progressions of 5 squares over quadratic fields: namely $\{i\}$ for $i=0,1,2$ and $\{i,j\}$ for $i=0,1$ and $j=1,\dots,4$ with $i<j$.

Lemma 3. *A non-constant arithmetic progression of five squares over a quadratic field, up to equivalence, is of type $\{3\}$.*

Proof. Let D be a squarefree integer and consider $x_0,\dots,x_4\in\mathbb{Q}(\sqrt{D})$ such that $x_0^2,\dots,x_4^2$ form a non-constant arithmetic progression. Without loss of generality we can assume that $x_n^2=a+nr$ for some $a,r\in\mathbb{Z}$ and $(x_n^2,x_m^2)=1$ if $n\neq m$.

Assume first that it is of type $\{i,j\}$, that is, $x_i^2=DX_i^2$, $x_j^2=DX_j^2$ and $x_k^2=X_k^2$ if $k\neq i,j$, where $X_n\in\mathbb{Z}$, $n=0,\dots,4$. Let $p>3$ be a prime dividing D. Since $(j-i)r=x_j^2-x_i^2=D(X_j^2-X_i^2)$, we have $p|r$, and therefore $p|a$. Thus we get that p divides x_n^2 for all $n=0,\dots,4$.

Let us see that, in fact, $p^2|x_n^2$ for all $n=0,\dots,4$, to obtain a contradiction (recall that x_n are not in $\mathbb{Z}$, so this is not automatic). Observe that for any $k\in\{0,\dots,4\}$ with $k\neq i,j$, we have that $x_k^2=X_k^2$ with $X_k\in\mathbb{Z}$, hence p divides X_k and so p^2 divides x_k^2. But now, considering $k,l\in\{0,\dots,4\}$ such that $k,l\neq i,j$ and $l>k$, we get that $(l-k)r=x_l^2-x_k^2$, and hence $p^2|r$, and therefore $p^2|a$. Then we have proved that the type $\{i,j\}$ is not possible over $\mathbb{Q}(\sqrt{D})$ for $|D|>3$. The remaining cases are not possible since there are not non-constant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$ for $D=-3,-2,-1,2$ and 3 (cf. [9]).

The type $\{1\}$ (or equivalently $\{5\}$) is not possible since there is not non-constant arithmetic progressions of four squares over the rationals.

To finish, let us see that the type $\{2\}$ is not possible. In this case we have that $[x_0:x_1:x_3:x_4]\in\mathbb{P}^3(\mathbb{Q})$ is a point on the intersection of two quadrics surface in $\mathbb{P}^3$:

$$C_{\{2\}}\;:\;\left\{\begin{array}{l} X_1^2+2X_4^2-3X_3^2=0\\ X_3^2+2X_0^2-3X_1^2=0.\end{array}\right.$$

Note that the eight points $[1:\pm1:\pm1:\pm1]$ belong to $C_{\{2\}}$. In the generic case the intersection of two quadric surfaces in $\mathbb{P}^3$ gives an elliptic curve and, indeed, this will turn out to be true in our case. A Weierstrass model for this curve is given by $E: y^2=x(x+1)(x+9)$ (this is denoted by `48A3` in Cremona's tables [7]). Using a computer algebra package like `MAGMA` or `SAGE` ([5], [12] resp.), we check that $E(\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$.

Therefore $C_{\{2\}} = \{[1 : \pm 1 : \pm 1 : \pm 1]\}$, which implies $x_n^2 = x_0^2$ for $n = 0, \dots, 4$. Thus is, $DX_2^2 = X_0^2$ which is impossible. □

Let D be a squarefree integer. We will denote by C_D the curve over $\mathbb{Q}$ that classify the arithmetic progressions of type $\{3\}$. As a consequence of the above result, we get the following geometric characterization.

Corollary 4. *Let D be a squarefree integer. Non-constant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{D})$, up to equivalences, are in bijection with the set $C_D(\mathbb{Q})$.*

The curve C_D has remarkable properties that we are going to show in the sequel. First of all, the curve C_D is a non singular curve over $\mathbb{Q}$ of genus 5 that can be given by the following equations in $\mathbb{P}^4$:

$$(1) \qquad C_D \ : \left\{ \begin{array}{l} F_{012} := X_0^2 - 2X_1^2 + X_2^2 = 0 \\ F_{123} := X_1^2 - 2X_2^2 + DX_3^2 = 0 \\ F_{234} := X_2^2 - 2DX_3^2 + X_4^2 = 0 \end{array} \right.$$

where we use the following convention: for $i, j, k \in \{0, \dots, 4\}$ distinct, F_{ijk} denotes the curve that classifies the arithmetic progressions $\{a_n\}_n$ (modulo equivalence) such that $a_i = d_i X_i^2$, $a_j = d_j X_j^2$, $a_k = d_k X_k^2$, where $d_i = 1$ if $i \neq 3$ and $d_3 = D$.

Observe that we could describe also the curve C_D by choosing three equations F_{ijk} with the only condition that all numbers from 0 to 4 appear in the subindex of some F_{ijk}.

We have 5 quotients of genus 1 that are the intersection of the two quadric surfaces in $\mathbb{P}^3$ given by $F_{ijk} = 0$ and $F_{ijl} = 0$, where $i, j, k, l \in \{0, \dots, 4\}$ distinct. Note that this quotients consist on removing the variable X_n, where $n \neq i, j, k, l$. We denote by $F_D^{(n)}$ to this genus 1 curve.

These curves are not in general elliptic curves over $\mathbb{Q}$, since they do not have always some rational point (except for $F^{(3)} := F_D^{(3)}$). But their jacobians are elliptic curves. A Weierstrass model of these elliptic curves can be computed by finding them in the case $D = 1$ (using that $F_1^{(i)}$ has always some easy rational point) and then twisting by D. Using the labeling of the Cremona's tables [7], one can check that $\mathrm{Jac}(F_D^{(0)})$ (resp. $\mathrm{Jac}(F_D^{(1)})$, $\mathrm{Jac}(F_D^{(2)})$, $\mathrm{Jac}(F_D^{(4)})$) is the D-twist of `24A1` (resp. `192A2`, `48A3`, `24A1`) and $\mathrm{Jac}(F^{(3)})$ is `192A2`. We denote by $E^{(0)}$ (resp. $E^{(1)}$, $E^{(2)}$) the elliptic curve `24A1` (resp. `192A2`, `48A3`) and by $E_D^{(i)}$ the D-twist of $E^{(i)}$, for $i = 0, 1, 2$. Observe also that $E^{(2)} = E_{-1}^{(0)}$, so $E_D^{(2)} = E_{-D}^{(0)}$.

Note that, in particular, we have shown the following result about the decomposition in the $\mathbb{Q}$-isogeny class of the jacobian of C_D.

Lemma 5. *Let D be a squarefree integer. Then*

$$\mathrm{Jac}(C_D) \stackrel{\mathbb{Q}}{\sim} \left(E_D^{(0)}\right)^2 \times E_D^{(2)} \times E_D^{(1)} \times E^{(1)}.$$

4. Local solubility for the curve C_D

The aim of this section is to describe under which conditions with respect to D the curve C_D has points in $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime numbers p.

Proposition 6. *Let D be a squarefree integer. Then C_D has points in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p if and only if $D > 0$, $D \equiv 1 \pmod{24}$, $D \equiv \pm 1 \pmod 5$ and for all primes p dividing D, $p \equiv 1 \pmod{24}$.*

This result is deduced from the following lemmata.

Lemma 7. *Let D be a squarefree integer. The curve C_D has points in K, for $K = \mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_3$ and $\mathbb{Q}_5$ if and only if D is square in K. Explicitly, $D > 0$, $D \equiv 1 \pmod 8$, $D \equiv 1 \pmod 3$ and $D \equiv \pm 1 \pmod 5$, respectively.*

Proof. First, suppose that D is a square over a field K. Then the curve C_D contains the following sixteen points $[1 : \pm 1 : \pm 1 : \pm\sqrt{D} : \pm 1]$. This shows one of the implications. In order to show the other implication we will consider the different fields separately. Suppose that $C_D(K) \neq \emptyset$.

If $K = \mathbb{R}$, the equation $F_{234} = 0$ implies that $2DX_3^2 = X_2^2 + X_4^2$, which has solutions in K only if $D > 0$.

Consider now the case $K = \mathbb{Q}_2$. On one hand, the conic given by the equation $F_{123} = X_1^2 - 2X_2^2 + DX_3^2$ has solutions in $\mathbb{Q}_2$ if and only if $(2, -D)_2 = 1$, where $(\ ,\ )_2$ denotes the Hilbert symbol. This last condition is equivalent to $D \equiv \pm 1 \pmod 8$ or $D \equiv \pm 2 \pmod{16}$. On the other hand, doing the same argument for the equation $F_{234} = X_2^2 - 2DX_3^2 + X_4^2$ we get the condition $(-1, 2D)_2 = 1$, which implies $D \equiv 1 \pmod 4$ or $D \equiv 2 \pmod 8$. So we get D odd and $D \equiv 1 \pmod 8$, or D even and $D \equiv 2 \pmod{16}$. This last case is equivalent, modulo squares, to the case $D = 2$ and it is easy to show that $C_2(\mathbb{Q}_2) = \emptyset$.

If $K = \mathbb{Q}_3$, considering the reduction modulo 3 of the conic given by the equation $F_{023} = 0$ we obtain that $D \not\equiv -1 \pmod 3$. Similarly, we have $D \not\equiv 0 \pmod 3$ using $F_{123} = 0$.

Finally if $K = \mathbb{Q}_5$, one can show just by an exhaustive search that there is no point in $C_D(\mathbb{F}_5)$ if $D \equiv \pm 2 \pmod 5$. The case $D \equiv 0 \pmod 5$ is discharged by using $F_{123} = 0$ modulo 5. □

In the following we will study the remaining primes $p > 5$ in two separate cases, depending if p divides or not D. The first observation is that the case that p does not divide D correspond to the good reduction case.

Lemma 8. *Let $p > 3$ be a prime does not divide D. Then C_D has good reduction on p given by the equations F_{012}, F_{123} and F_{234}.*

Proof. We use the jacobian criterium. The Jacobian matrix of the system of equations defining C_D is

$$A := (\partial F_{i(i+1)(i+2)}(X_i, X_{i+1}, X_{i+2})/\partial X_j)_{0 \le i \le 2, 0 \le j \le 4}.$$

For any $j_1 < j_2$, denote by A_{j_1,j_2} the square matrices obtained from A by deleting the columns j_1 and j_2. Their determinant is equal to

$$|A_{j_1,j_2}| = k_{j_1,j_2} \cdot \prod_{i \neq j_1, j_2} X_i$$

where

$$k_{0,1} = 2^3 D\ ,\ k_{0,2} = -2^4 D\ ,\ k_{0,3} = 2^3 3\ ,\ k_{0,4} = 2^5 D\ ,\ k_{1,2} = 2^3 D,$$
$$k_{1,3} = -2^4\ ,\ k_{1,4} = 2^3 3D\ ,\ k_{2,3} = 2^3\ ,\ k_{2,4} = -2^4 D\ ,\ k_{3,4} = 2^3.$$

Now, suppose we have a singular point of $C_D(\mathbb{F}_p)$. Then the matrix A must have rank less than 3 evaluated at this point, so all these determinants must be 0. But, if $p > 3$ and does not divide D, then all the products of their homogeneous coordinates must be zero, so the point must have three coordinates equal to 0, which is impossible again if $p > 3$. □

Lemma 9. *Let $p > 5$ be a prime such that p does not divide D. Then $C_D(\mathbb{Q}_p) \neq \emptyset$.*

Proof. First of all, by Hensel's lemma, and since C_D has good reduction at p, we have that any solution modulo p lifts to some solution in $\mathbb{Q}_p$. So we only need to show that $C_D(\mathbb{F}_p) \neq \emptyset$. Now, because of the Weil bounds, we know that $\sharp C_D(\mathbb{F}_p) > p + 1 - 10\sqrt{p}$. So, if $p > 97$, then $C_D(\mathbb{F}_p) \neq \emptyset$ and we are done. For the rest of primes p, $5 < p < 97$, an exhaustive search proves the result. □

We suspect that there should be some reason, besides the Weil bound, that for all primes $p > 5$ not dividing D, the curve C_D has points modulo p, that should be related to the special form it has or to the moduli problem it classifies.

Lemma 10. *Let p be a prime dividing D, and $p > 3$. Then $C_D(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 1 \pmod{24}$.*

Proof. We will show that a necessary and sufficient condition for $C_D(\mathbb{Q}_p) \neq \emptyset$ is that 2, 3 and -1 are all squares in $\mathbb{F}_p$. This happens exactly when $p \equiv 1 \pmod{24}$. Note that this condition is sufficient since $[\sqrt{3} : \sqrt{2} : 1 : 0 : \sqrt{-1}]$ belongs to C_D.

Suppose that we have a solution $[x_0 : x_1 : x_2 : x_3 : x_4]$, with $x_i \in \mathbb{Z}_p$, and such that not all of them are divisible by p. The first observation is that only one of the x_i can be divisible by p; since if two of them, x_i and x_j, are divisible by p, we can use the equations F_{ijk} in order to show that x_k is also divisible, for any k.

Now, reducing F_{123} modulo p, we get that 2 must be a square modulo p. Reducing F_{234} modulo p we get that -1 must be a square modulo p. And finally, reducing $F_{034} = X_0^2 - 4DX_3^2 + 3X_4^2$ modulo p we get that 3 must be a square modulo p. So the conditions are necessary. □

5. The rank condition

Let us start recalling the well-known 2-descent on elliptic curves, as explained for example in [11, Chapter X, Prop. 1.4]. Consider E an elliptic curve over a number field K given by an equation of the form

$$y^2 = x(x - e_1)(x - e_2) \ , \quad \text{with } e_1, e_2 \in K.$$

Let S be the set of all archimedean places, all places dividing 2 and all places where E has bad reduction. Let $K(S, 2)$ be the set of all elements b in K^*/K^{*2} with $\operatorname{ord}_v(b) = 0$ for all $v \notin S$. Given any $(b_1, b_2) \in K(S, 2) \times K(S, 2)$, define the curve H_{b_1,b_2} given as intersection of two quadrics in $\mathbb{P}^3$ by the equations

$$H_{b_1,b_2} : \begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_1 z_0^2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_2 z_0^2. \end{cases}$$

Then the curves H_{b_1,b_2} have genus one with Jacobian E, and we have a natural degree four map $\phi_{b_1,b_2} : H_{b_1,b_2} \to E$ given by

$$\phi_{b_1,b_2}(z_0, z_1, z_2, z_3) := (b_1(z_1/z_0)^2, b_1 b_2 z_1 z_2 z_3/z_0^3).$$

Moreover, the 2-Selmer group $S^{(2)}(E/K)$ of E can be identified with the subset

$$S^{(2)}(E/K) = \{(b_1, b_2) \in K(S,2) \times K(S,2) \mid H_{b_1,b_2}(K_v) \neq \emptyset \ \forall v \text{ place in } K\}.$$

The group $E(K)/2E(K)$ can be described, via the natural injective map $\psi : E(K)/2E(K) \to S^{(2)}(E/K)$ defined by

$$\psi((x,y)) = \begin{cases} (x, x-e_1) & \text{if} \quad x \neq 0, e_1 \\ (e_2/e_1, -e_2) & \text{if} \quad (x,y) = (0,0) \\ (e_1, -e_2/e_1) & \text{if} \quad (x,y) = (e_1, 0) \end{cases}$$

and $\psi(0) = (1,1)$, with the subgroup consisting of $(b_1, b_2) \in K(S,2) \times K(S,2)$ such that $H_{b_1,b_2}(K_v) \neq \emptyset$.

The following lemma is elementary by using the description above, an it is left to the reader.

Lemma 11. *Let H be a genus 1 curve over a number field K given by an equation of the form*

$$H : \begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_1 z_0^2 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_2 z_0^2 \end{cases}$$

for some $b_1, b_2, e_1, e_2 \in K$. Let $D \in K^*$ and consider the curves $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ given by changing z_1^2 by Dz_1^2, z_2^2 by Dz_2^2 and z_3^2 by Dz_3^2 respectively in the equations above. Then $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ are homogeneous spaces for the elliptic curve E_D, the twist by D of E, given by the Weierstrass equation $y^2 = x(x - De_1)(x - De_2)$.

Moreover, if S_D denotes the set of all archimedean places, all places dividing $2D$ and all places where E has bad reduction, the curves $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ correspond respectively to the elements (Db_1, b_2), (b_1, Db_2) and (Db_1, Db_2) in $K(S_D,2) \times K(S_D,2)$.

Proposition 12. *Let $D > 0$ be a squarefree integer. A necessary condition for the existence of 5 non-trivial squares in arithmetic progression over $\mathbb{Q}(\sqrt{D})$ is that the elliptic curves $E_D^{(0)}$ and $E_D^{(2)}$ given by equations $Dy^2 = x(x+1)(x+4)$ and $Dy^2 = x(x+1)(x+9)$ have rank 2 or larger over $\mathbb{Q}$, and that the elliptic curve $E_D^{(1)}$ given by the equation $Dy^2 = x(x+2)(x+6)$ has an infinite number of rational solutions.*

Proof. Assume we have 5 non-trivial squares in arithmetic progression over $\mathbb{Q}(\sqrt{D})$. By using the results of section 3, we can assume that such squares are of the form x_0^2, x_1^2, x_2^2, Dx_3^2 and x_4^2, with $x_i \in \mathbb{Z}$. The condition of being in arithmetic progression is equivalent to $x_0^2 = a$ $x_1^2 = a + q$, $x_2^2 = a + 2q$, $Dx_3^2 = a + 3q$ and $x_4^2 = a + 4q$ for some $a, q \in \mathbb{Z}$. From these equations we easily get that the following homogeneous spaces attached to $E_D^{(0)}$ have rational points:

$$\begin{cases} 2(DX_3)^2 - 3DX_2^2 = -DX_0^2 \\ 2(DX_3)^2 - 6DX_1^2 = -4DX_0^2 \end{cases} \quad \text{and} \quad \begin{cases} 2DX_4^2 - 3(DX_3)^2 = -DX_1^2 \\ 2DX_4^2 - 6DX_2^2 = -4DX_1^2 \end{cases}$$

which give $(2, 3D)$ and $(2D, 3) \in S^{(2)}(E_D^{(0)}/\mathbb{Q})$ by using Lemma 11. Since we are supposing both curves have points in $\mathbb{Q}$, they correspond to two points P_1 and P_2 in $E_D^{(0)}(\mathbb{Q})$. In

order to show they have infinite order, we only need to show that the symbols $(2, 3D)$ and $(2D, 3)$ are not in

$$\psi(E_D^{(0)}[2]) = \{(1,1), (4,4D) = (1,D), (-D,-1), (-D,-D)\}$$

which is clear since $D > 0$. In order to show that P_1 and P_2 are independent modulo torsion, it is sufficient to show that $(2, 3D)(2D, 3) = (D, D)$ is not in $\psi(E_D^{(0)}[2])$, which is clear again. So $E_D^{(0)}(\mathbb{Q})$ has rank > 1.

The other conditions appear similarly. We have that

$$\begin{cases} 3DX_4^2 - 4(DX_3)^2 = -DX_0^2 \\ 3DX_4^2 - 12DX_1^2 = -9DX_0^2 \end{cases} \quad \text{and} \quad \begin{cases} 3DX_0^2 - 4DX_1^2 = -DX_4^2 \\ 3DX_0^2 - 12D^2X_3^2 = -9DX_4^2 \end{cases}$$

which give $(3D, 1)$ and $(3D, 4D) = (3D, D) \in S^{(2)}(E_D^{(2)}/\mathbb{Q})$, giving again two independent points in $E_D^{(2)}(\mathbb{Q})$.

Finally, we have that

$$6DX_4^2 - 2(2DX_3)^2 = -2DX_0^2 \ , \ 6DX_4^2 - 12DX_1^2 = -6DX_0^2$$

which gives $(6D, 2) \in S^{(2)}(E_D^{(1)}/\mathbb{Q})$, giving a non torsion point in $E_D^{(1)}(\mathbb{Q})$. $\square$

Remark 13. Suppose that D verifies the conditions in Proposition 6, so $C_D(\mathbb{Q}_p) \neq \emptyset$ for all p. Then the root number of $E_D^{(0)}$ and $E_D^{(2)}$ is 1 independently of D in both cases, and the root number of $E_D^{(1)}$ is always -1. This is because the root number of the twist by D of an elliptic curve E of conductor N, if N and $D > 0$ are coprime, is equal to the Legendre symbol $(D/-N)$ times the root number of E (see for example the Corollary to Proposition 10 in [10]). In our case, and assuming D verifies the conditions in Proposition 6, we get that the root number of $E_D^{(i)}$ is equal to the root number of $E^{(i)}$, since $(D/-N) = 1$ for $N = 24, 48, 192$.

Assuming the so called Parity conjecture, this implies that the rank of $E_D^{(0)}$ and $E_D^{(2)}$ is always even, and the rank of $E_D^{(1)}$ is always odd. So the last condition in the proposition is (conjecturally) empty.

Ternary Quadratic Forms. It has been showed at Proposition 12 that a necessary condition to the existence of a non-constant arithmetic progression of 5 squares over a quadratic field $\mathbb{Q}(\sqrt{D})$ is that the elliptic curve $E_D^{(0)}$ and $E_D^{(2)}$ have positive even ranks. In this part we want to describe some explicit results concerning the ranks of these curves, obtaining hence some explicit computable condition.

Remark 14. The elliptic curve $E_D^{(0)}$ (resp. $E_D^{(2)}$) parametrizes non-constant arithmetic progression of 4 squares over $\mathbb{Q}(\sqrt{D})$ (resp. $\mathbb{Q}(\sqrt{-D})$) (cf. [9]). Therefore a necessary condition to the existence of a non-constant arithmetic progression of 5 squares over $\mathbb{Q}(\sqrt{D})$ is the existence of a non-constant arithmetic progression of 4 squares over $\mathbb{Q}(\sqrt{D})$ and over $\mathbb{Q}(\sqrt{-D})$.

Using Waldspurger's results and Shimura's correspondence *a la* Tunnell, Yoshida [14] obtained several results on the ranks of $E_D^{(0)}$ and $E_D^{(2)}$. In particular, we use his results corresponding to the case $D \equiv 1 \pmod{24}$ to apply it to our problem.

Proposition 15. *Let D be a squarefree integer. If $Q(x,y,z)\in\mathbb{Z}[x,y,z]$ is a ternary quadratic forms, denote by $r(D,Q(x,y,z))$ the number of integer representations of D by Q. If*

$$\begin{array}{rcl} r(D,x^2+12y^2+15z^2+12yz) & \neq & r(D,3x^2+4y^2+13z^2+4yz) \\ & or & \\ r(D,x^2+3y^2+144z^2) & \neq & r(D,3x^2+9y^2+16z^2), \end{array}$$

then there are not non-constant arithmetic progressions of 5 squares over $\mathbb{Q}(\sqrt{D})$.

Proof. First of all, by the Proposition 6 we have that $D\equiv 1 \pmod{24}$. Now, Yoshida constructs two cuspidal forms of weight 3/2 denoted by $\Phi_{3,-3}$ and $\Phi_{1,1}$ such that if we denote by $a_D(\Phi_{3,-3})$ (resp. $a_D(\Phi_{1,1})$) the D-th coefficient of the Fourier q-expansion of $\Phi_{3,-3}$ (resp. $\Phi_{1,1}$), we have

$$a_D(\Phi_{3,-3})=0 \text{ if and only if } L(E_D^{(0)},1)=0,$$
$$a_D(\Phi_{1,1})=0 \text{ if and only if } L(E_D^{(2)},1)=0.$$

Then by the definition of these cuspidal forms we have:

$$\begin{aligned} a_D(\Phi_{3,-3}) &= r(D,x^2+12y^2+15z^2+12yz)-r(D,3x^2+4y^2+13z^2+4yz)\,, \\ a_D(\Phi_{1,1}) &= r(D,x^2+3y^2+144z^2)-r(D,3x^2+9y^2+16z^2)\,, \end{aligned}$$

which finishes the proof. □

Remark 16. For $D=2521$, the conditions in Propositions 6, 12 and 15 are fulfilled, an in fact all the revelant genus 1 curves have rational points. But we will show in Corollary 33 that $C_{2521}(\mathbb{Q})=\emptyset$.

6. The Mordell-Weil sieve

In this section we want to develop a method to test when C_D has no rational points. Contrary to the test given before, the one we construct gives conjecturally always the right answer; i.e., if the curve has no rational points, then it does not pass the test.

The idea is the following: Suppose we have a curve C defined over a number field K together with a map $\phi: C\to A$ to an abelian variety A defined over K. We want to show that $C(K)=\emptyset$, and we know that $\phi(C(K))\subset H\subset A(K)$, a certain subset of $A(K)$. Let $\wp$ be a prime of K and consider the reduction at $\wp$ of all the objects $\phi_\wp: C_\wp\to A_\wp$, together with the reduction maps $\mathrm{red}_\wp: A(K)\to A(k_\wp)$, where $k_\wp$ is the residue field at $\wp$. Now, we have that $\mathrm{red}_\wp(C(K))\subset\phi_\wp(C(k_\wp))\cap\mathrm{red}_\wp(H)$, so

$$\phi(C(K))\subset H^{(\wp)}:=\mathrm{red}_\wp^{-1}\Big(\phi_\wp(C(k_\wp))\cap\mathrm{red}_\wp(H)\Big).$$

By considering sufficiently many primes, it could happen that

$$\bigcap_{\text{some primes } \wp} H^{(\wp)}=\emptyset,$$

getting that $C(K)=\emptyset$.

In our case, we consider the curve C_D together with a map $\phi: C_D\to E^{(1)}$, where $E^{(1)}$ is the curve given by the Weierstrass equation $y^2=x(x+2)(x+6)$. The curve $E^{(1)}$ has Mordell-Weil group $E^{(1)}(\mathbb{Q})$ generated by the 2-torsion points and $P:=(6,24)$.

Lemma 17. *Let D be a squarefree integer, and consider the curve C_D, together with the map $\phi : C_D \to E^{(1)}$ defined as*

$$\phi([x_0 : x_1 : x_2 : x_3 : x_4]) := \left(\frac{6x_0^2}{x_4^2}, \frac{24x_0x_1x_2}{x_4^3}\right).$$

Let $P := (6, 24) \in E^{(1)}(\mathbb{Q})$. Then

$$\phi(C_D(\mathbb{Q})) \subset H := \{kP \mid k \text{ odd }\}.$$

Proof. This lemma is an easy application of the 2-descent. The map ϕ is the composition of two maps. First, the forgetful map from C_D to the genus one curve in $\mathbb{P}^3$ given by the equations

$$\begin{cases} F_{014} := 3X_0^2 - 2X_1^2 + 2X_4^2 = 0, \\ F_{024} := X_0^2 - 2X_2^2 + X_4^2 = 0, \end{cases}$$

given by sending $[x_0 : x_1 : x_2 : x_3 : x_4]$ to $[x_0 : x_1 : x_2 : x_4]$. Multiplying F_{014} by 2 and F_{024} by 6 we get the equations of a 2-descendent

$$\begin{cases} 6X_0^2 - 2(2X_1)^2 = -2X_4^2, \\ 6X_0^2 - 12X_2^2 = -6X_4^2. \end{cases}$$

The second map is the corresponding 4 degree map $\phi_{6,2}$ from these curve to $E^{(1)}$ given by the equations above, and determining the element $(6, 2) \in S^{(2)}(E^{(1)}/\mathbb{Q})$, so $\phi(C_D(\mathbb{Q}))$ is contained in the subset of elements (x, y) of $E^{(1)}(\mathbb{Q})$ with $\psi((x, y)) := (x, x + 2) = (6, 2)$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. But $P := (6, 24) \in E^{(1)}(\mathbb{Q})$ is a generator of $E^{(1)}(\mathbb{Q})/E^{(1)}(\mathbb{Q})[2]$, and has $\psi(6, 24) = (6, 2)$, hence any such point (x, y) is an odd multiple of P. □

For any prime q, we will denote by $H_D^{(q)} \subset H$ the subset corresponding to

$$H_D^{(q)} := \mathrm{red}_q^{-1}\left(\phi_q(C_D(\mathbb{F}_q)) \cap \mathrm{red}_q(H)\right).$$

First, consider the reduction modulo a prime q dividing D, so a prime not of good reduction. Suppose we have a solution $[x_0 : x_1 : x_2 : x_3 : x_4]$ of C_D, so x_0^2, x_1^2, x_2^2, Dx_3^2 and x_4^2 are coprime integers in arithmetic progression. By doing modulo q one gets that x_0^2, x_1^2, x_2^2, 0 and x_4^2 are in arithmetic progression modulo q, so, after dividing by x_4^2, we can suppose it is the arithmetic progression $-3, -2, -1, 0, 1$.

Proposition 18. *Let $q > 3$ be a prime number dividing D. Then*

$$H_D^{(q)} = \{kP \mid k \text{ odd and } x(kP) \equiv -18 \pmod{q}\},$$

and $H_D^{(q)}$ is independent on D.

Proof. These is an easy application of the ideas above. Since the only points in the reduction of C_D are the ones having $x_0^2 = -3$, $x_1^2 = -2$, $x_2^2 = -1$ and $x_4^2 = 1$, the set $\phi_q(C_D(\mathbb{F}_q))$ contains only at most the two points having x-coordinate equal to $6(-3) = -18$. □

Corollary 19. *Suppose that $q > 3$ is a prime number such that $\mathrm{red}_q(H)$ contains a point Q with $x(Q) \equiv -18 \pmod{q}$. Then there exists infinitely many pairs of squarefree integers D and primitive tuples $[x_0 : x_1 : x_2 : x_3 : x_4] \in C_D(\mathbb{Q})$ such that either q divides D or $x_3 \equiv 0 \pmod{q}$.*

Proof. Let O_q be the order of P modulo q, and let k be such that $x(kP) \equiv -18 \pmod{q}$. Then $x(k'P) \equiv -18 \pmod{q}$ for all $k' \equiv k \pmod{O_q}$. So, if k is odd or O_q is odd, $H^{(q)}$ has infinite elements. For any point $Q \in H^{(q)}$, we have that $x(Q) = 6z^2$ for certain $z \in \mathbb{Q}$ and such that $z^2 \equiv -3 \pmod{q}$. Write $z = a/b$ with a and $b \in \mathbb{Z}$ and coprime. Then, if we denote by $r := (a^2 - b^2)/4$, then $r \in \mathbb{Z}$ and $x_i := a^2 + ir$ are squares for $i = 0, 1, 2$ and 4, and $a^2 + 3r \equiv 0 \pmod{q}$. Define D the squarefree part of $a^2 + 3r$, we get the result by defining x_3 such that $a^2 + 3r = D'x_3^2$. $\square$

Observe, however, that we do not get that $C_q(\mathbb{Q}) \neq \emptyset$ for the primes satisfying the hypothesis of the above corollary. For example, the prime $q = 457$ verifies the conditions of the corollary, but we will show that $C_{457}(\mathbb{Q}) = \emptyset$.

Now we will consider primes $q > 3$ that do not divide D, hence good reduction primes. We will obtain conditions depending on D being a square or not modulo q.

Proposition 20. *Let $q > 3$ be a prime number not dividing D. Then $H_D^{(q)} \subset E^{(1)}(\mathbb{Q})$ depends only on the Legendre symbol (D/q). If we denote by $H^{(q),(D/q)}$ the subgroup corresponding to any (D/q), and by O_q the order of $P \in E^{(1)}(\mathbb{Q})$ modulo q, we have that there exists subsets $M_1^{(q)}$ and $M_{-1}^{(q)}$ of $\mathbb{Z}/O_q\mathbb{Z}$ such that*

$$H^{(q),(D/q)} = \{kP \mid k \text{ odd and } \exists m \in M_{(D/q)}^{(q)} \text{ such that } k \equiv m \pmod{O_P}\}.$$

Moreover, $1 \in M_1^{(q)}$ for any $q > 3$, and if $k \in M_{(D/q)}^{(q)}$, then $-k \in M_{(D/q)}^{(q)}$.

Proof. First we show that $H_D^{(q)}$ only depends on (D/q). Suppose that $D \equiv D'a^2 \pmod{q}$, for certain $a \neq 0 \in \mathbb{F}_q$. Then the morphism given by $\theta([x_0 : x_1 : x_2 : x_3 : x_4]) = [x_0 : x_1 : x_2 : x_3 a^2 : x_4]$ determines an isomorphism between $C_{D'}$ and C_D defined over $\mathbb{F}_q$ and clearly commuting with ϕ, which does not depend on the x_3.

In order to define $M_{(D/q)}^{(q)}$, one computes $\phi_q(C_D(\mathbb{F}_q))$ and then intersect with the subset of $E^{(1)}(\mathbb{F}_q)$ of the form $\{kP \mid k \text{ odd }\}$. Then

$$M_{(D/q)}^{(q)} := \{k \in \mathbb{Z}/O_q\mathbb{Z} \mid kP \in \phi_q(C_D(\mathbb{F}_q))\}.$$

So k belongs to $M_{(D/q)}^{(q)}$ if there exists some $Q := [x_0 : x_1 : x_2 : x_3 : x_4] \in C_D(\mathbb{F}_q)$ such that $\phi(Q) = kP$. But then $\phi([-x_0 : x_1 : x_2 : x_3 : x_4]) = -kP$.

Finally, if $(D/q) = 1$, we can suppose $D \equiv 1 \pmod{q}$. But then $Q_0 := [1 : 1 : 1 : 1 : 1] \in C_D(\mathbb{F}_q)$, and $\phi(Q_0) = P$. $\square$

The following table shows some examples of $M_{\pm 1}^{(q)}$ for $5 < q < 30$ prime.

q	O_q	$M_1^{(q)}$	$M_{-1}^{(q)}$
7	6	$\{\pm 1\}$	$\{3\}$
11	8	$\{\pm 1\}$	$\{\pm 3\}$
13	6	$\{\pm 1\}$	$\{3\}$
17	6	$\{\pm 1, 3\}$	$\{\ \}$
19	8	$\{\pm 1\}$	$\{\pm 3\}$
23	3	$\{1, 2, 3\}$	$\{\ \}$
29	16	$\{\pm 1\}$	$\{\pm 3, \pm 5, \pm 7\}$

We are going to use the above result to obtain conditions on D.

Corollary 21. *If $C_D(\mathbb{Q}) \neq \emptyset$ then D satisfies the following conditions:*

(i) *D is a square modulo 17, 23, 41, 191, 281, 2027, 836477.*

(ii) $(D/7) = (D/13)$, $(D/11) = (D/19) = (D/241)$, $(D/47) = (D/73)$, $(D/149) = (D/673)$, $(D/43) = (D/1723)$, $(D/175673) = (D/2953)$, $(D/97) = (D/5689) = (D/95737)$, $(D/577) = (D/2281)$, $(D/83) = (D/4391) = (D/27449)$, $(D/67) = (D/136319)$, $(D/2111) = (D/2521)$.

(iii) *If* $(D/29) = 1$ *then* $(D/11) = 1$. *If* $(D/149) = 1$ *then* $(D/31) = 1$. *If* $(D/7019) = 1$ *then* $(D/8123) = 1$. *If* $(D/617) = 1$ *then* $(D/37) = 1$, *and in this case* $(D/7) = 1$.

(iv) *If* $(D/83) = -1$ *then* $(D/11) = -1$. *If* $(D/2347) = -1$ *then* $(D/47) = -1$. *If* $(D/10369) = -1$ *then* $(D/47) = -1$.

Proof. We have computed the sets $M_1^{(q)}$ and $M_{-1}^{(q)}$ for $q < 10^6$ and $O_q \leq 200$. Then the algorithm to obtain the conditions of the statement is as follow: fix an integer $k \leq 200$ and compute the primes q such that $O_q = k$ and $5 < q < 10^6$. For these primes compute $M_1^{(q)}$ and $M_{-1}^{(q)}$. If $M_{-1}^{(q)}$ is empty then $(D/q) = 1$ and we get (i). If these sets are equal for different primes then we obtain (ii). Now for any integer $m > 1$ such that $mk \leq 200$ compute the primes $p < 10^6$ such that $O_p = mk$. Compute $M_1^{(p)}$ and $M_{-1}^{(p)}$. Now check if $M_1^{(p)}$ (resp. $M_{-1}^{(p)}$) mod k is equal to some of the sets $M_1^{(q)}$ (resp. $M_{-1}^{(q)}$) computed above. If that happens then we obtain the rest of the conditions.

For example looking at the table above we see that $M_{-1}^{(17)} = \{\}$, therefore $(D/17) = 1$. Now, $O_7 = O_{13}$, $M_1^{(7)} = M_1^{(13)}$ and $M_{-1}^{(7)} = M_{-1}^{(13)}$ so we have $(D/7) = (D/13)$. Finally, $O_{29} = 2O_{11}$ and $M_1^{(29)}$ mod O_{11} is equal to $M_1^{(11)}$ and then we get that if $(D/29) = 1$ then $(D/11) = 1$. □

7. Computing all the points for $D = 409$

We want to find all the rational points of the curve C_D when we know there are some. We will concentrate at the end in the case $D = 409$, which is the first number that pass all the test (see Corollary 33), but for the main part of the section we can suppose D is any prime integer verifying the conditions in Proposition 6. Observe first that we do have the 16 rational points $[\pm 7, \pm 13, \pm 17, 1, \pm 23] \in C_{409}(\mathbb{Q})$. Our aim is to show that there are no more.

In recent years, some new techniques have been developed in order to compute all the rational points of a curve of genus greater than one over $\mathbb{Q}$. These techniques work only under some special hypothesis. For example, Chabauty's method can be used when the Jacobian of the curve have rank less than the genus of the curve, or even when there is a quotient abelian variety of the jacobian with rank less than its dimension. In our case, however, the jacobian of the curve C_D is isogenous to a product of elliptic curves, each of then with rank one or higher (in fact, the jacobian of C_D must have rank ≥ 8 by Proposition 12). So we cannot apply these method. Other methods, like the Manin-Drinfeld's method, cannot be applied either. We will instead apply the covering collections technique, as developed by Coombes and Grant [6], Wetherell [15] and others, and specifically a modification of what is now called the elliptic Chabauty method developed by Flynn and Wetherell in [8] and by Bruin in [3].

The idea is as follows: suppose we have a curve C over a number field K and an unramified map $\chi : C' \to C$ of degree greater than one and defined over K. We consider the distinct unramified coverings $\chi^{(s)} : C'^{(s)} \to C$ formed by twists of the given one, and we get that

$$C(K) = \bigcup_s \chi^{(s)}(C'^{(s)}(K)),$$

the union being disjoint. In fact, only a finite number of twists do have rational points, and the finite (larger) set of twists having points locally everywhere can be explicitly described. Now one hopes to be able to compute the rational points of all the curves $C'^{(s)}$, so also of the curve C.

We will consider degree 2 coverings (which could not exists over $\mathbb{Q}$). To construct such coverings, we will use the description given by Bruin and Flynn in [4] of the 2-coverings of hyperelliptic curves. Our curve C_D is not hyperelliptic, but a quotient of itself it is, so we will use a 2-covering of such quotient. Specifically, we will use one of the five genus 1 quotients, concretely the quotient

$$F_D^{(4)} : DX_3^2 = t^4 - 8t^3 + 2t^2 + 8t + 1\,,$$

together with the forgetful map $\phi^{(4)} : C_D \longrightarrow F_D^{(4)}$ given by $t = \frac{X_0 - X_1}{X_2 - X_1}$.

Observe first that the curve C_D has some $\mathbb{Q}$-defined automorphisms τ_i of order 2, defined by sending $\tau_i(x_j) = x_j$ if $j \neq i$, $\tau_i(x_i) = -x_i$. All them, together with their compositions, form a subgroup Υ of the automorphisms isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. For every $\mathbb{Q}$-defined point of C_D, composing with these automorphisms gives 16 different points. Given $Q \in C_D(\mathbb{Q})$, we denote by T_Q the set of all this 16 diferent point. Observe that $\phi^{(4)}(T_Q)$ is formed by 8 distinct points.

Lemma 22. *The involutions τ_0, τ_1, τ_2 and τ_3 give the following involutions on $F_D^{(4)}$:*

$$\tau_0(t, X_3) = \left(\frac{1-t}{1+t}, \frac{2X_3}{(1+t)^2}\right),\ \tau_1(t, X_3) = \left(\frac{-1}{t}, \frac{X_3}{t^2}\right),\ \tau_2(t, X_3) = \left(\frac{t+1}{t-1}, \frac{2X_3}{(t-1)^2}\right),$$

and $\tau_3(t, X_3) = (t, -X_3)$. Moreover, if $F_D^{(4)}(\mathbb{Q}) \neq \emptyset$ and $\psi : F_D^{(4)} \to E_D^{(0)}$ is an isomorphism, then the involutions of $E_D^{(0)}$ given by $\epsilon_i := \psi\tau_i\tau_3\psi^{-1}$ for $i = 0, 1, 2$, are independent of ψ. Specifically, $\epsilon_i = \epsilon_{R_i}$ for $R_0 = (0, 0)$, $R_1 = (-D, 0)$ and $R_2 = (-4D, 0)$, where ϵ_Q denotes the translation by $Q \in E_D^{(0)}$.

Proof. It is a straightforward computation to check the formulae for the involutions on $F_D^{(4)}$.

First, we show that the involutions ϵ_i are independent of the fixed isomorphism ψ. In order to show this, recall that, in any elliptic curve, any involution ϵ that has no fixed points should be of the form $\epsilon_R(S) = S + R$, for a fixed 2-torsion point R. Since $\tau_i\tau_3$ has no fixed points in $F_D^{(4)}$, their corresponding involution ϵ_i in $E_D^{(0)}$ must be equal to some ϵ_{R_i}, hence determined by the corresponding 2-torsion point R_i, which is equal to $\epsilon_i(0)$. Now, changing the isomorphism ψ from $F_D^{(4)}$ to $E_D^{(0)}$ is equivalent to conjugate ϵ_i by a translation ϵ_Q of $E_D^{(0)}$ with respect to a point Q in $E_D^{(0)}$, so we get in principle a new involution $\epsilon_{-Q}\epsilon_i\epsilon_Q$, again without fixed points. But $\epsilon_{-Q}\epsilon_i\epsilon_Q(0) = \epsilon_{-Q}(\epsilon_i(Q)) = \epsilon_{-Q}(Q + R_i) = R_i$, so $\epsilon_{-Q}\epsilon_i\epsilon_Q = \epsilon_i$.

Second, since ϵ_i is independent of the chosen isomorphism ψ, and also does not depend on the field K, we can change to a field $K' := K(\sqrt{D})$ where we have $F_D^{(4)} \cong F_1^{(4)}$, so we are reduced to the case $D = 1$. In this case, a simple computation by choosing some point in $F_1^{(4)}(\mathbb{Q})$ shows that $\epsilon_i = \epsilon_{R_i}$ where $R_0 = (0,0)$, $R_1 = (-1,0)$ and $R_2 = (-4,0)$ in $E_1^{(0)}$, which give the result when we translate them to the curve $E_D^{(0)}$. □

Now, we want to construct some degree two unramified coverings of $F_D^{(4)}$. All these coverings are, in this case, defined over $\mathbb{Q}$, but we are interested in special equations not defined over $\mathbb{Q}$. The idea is easy: first, factorize the polinomial $q(t) := t^4-8t^3+2t^2+8t+1$ as the product of two degree 2 polynomials (over some quadratic extension K). In the sequel of this section, we will denote $K := \mathbb{Q}(\sqrt{2})$. Then we have the factorization $q(t) = q_1(t)q_2(t)$ over K where $q_1(t) := t^2 - (4+2\sqrt{2})t - 3 - 2\sqrt{2}$ and $q_2(t) := \overline{q_1}(t)$, where $\overline{z}$ denotes the Galois conjugate of $z \in K$ over $\mathbb{Q}$. We could have chosen other factorizations over other quadratic fields, but this one is especially good for our purposes as we will show in the sequel. Then, for any $\delta \in K$, the curves F'_δ defined in $\mathbb{A}^3$ by the equations

$$F'_\delta : \begin{cases} \delta y_1^2 &= q_1(t) = \quad t^2 - (4+2\sqrt{2})t - 3 - 2\sqrt{2} \\ (D/\delta) y_2^2 &= q_2(t) = \quad t^2 - (4-2\sqrt{2})t - 3 + 2\sqrt{2} \end{cases}$$

together with the map ν_δ that gives $X_3 = y_1 y_2$ are all the twists of an unramified degree two coverings of $F_D^{(4)}$. Observe that, for any δ and δ' such that $\delta\delta'$ is a square in K, we have an isomorphism between F'_δ and $F'_{\delta'}$. So we need to consider only the δ's modulo squares. This also means that we can suppose that $\delta \in \mathbb{Z}[\sqrt{2}]$. However, only very few of them are necessary in order to cover all the rational points of $F_D^{(4)}$. A method to show this type of results is explained in [4], but we will follow a different approach.

Lemma 23. *Let $D > 3$ be a prime number such that $F_D^{(4)}(\mathbb{Q}) \neq \emptyset$. Let $\alpha \in \mathbb{Z}[\sqrt{2}]$ be such that $\nu_\alpha(F'_\alpha(K)) \cap F_D^{(4)}(\mathbb{Q}) \neq \emptyset$, then*

$$F_D^{(4)}(\mathbb{Q}) \subset \nu_\alpha(F'_\alpha(K)) \cup \nu_{\overline{\alpha}}(F'_{\overline{\alpha}}(K)) \cup \nu_{-\alpha}(F'_{-\alpha}(K)) \cup \nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K)).$$

Moreover, for any $Q \in C_D(\mathbb{Q})$, either

$$\phi^{(4)}(T_Q) \cap \nu_\alpha(F'_\alpha(K)) \neq \emptyset \quad \text{or} \quad \phi^{(4)}(T_Q) \cap \nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K))) \neq \emptyset.$$

Proof. Observe that, for any point $P \in F_D^{(4)}$, an easy calculation shows that

$$q_1(t(\tau_0(P))) = \frac{2}{(1+t(P))^2} q_1(t(P)) \text{ and } q_1(t(\tau_1(P))) = -\frac{(1+\sqrt{2})^2}{(t(P))^2} q_2(t(P)),$$

where $t(R)$ denotes the t-coordinate of the point R. This implies that, if P is in $\nu_\alpha(F'_\alpha(K)) \cap F_D^{(4)}(\mathbb{Q})$, then $\tau_0(P)$ and $\tau_3(P)$ also are, and $\tau_1(P)$ and $\tau_2(P)$ are in $\nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K)) \cap F_D^{(4)}(\mathbb{Q})$. This last fact shows the last assertion of the lemma.

Now, using a fixed point $P \in F_D^{(4)}(\mathbb{Q})$, we choose $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $P \in \nu_\alpha(F'_\alpha(K))$, and an isomorphism ψ_P of $F_D^{(4)}$ with its jacobian $E := E_D^{(0)}$, by sending P to 0 (this isomorphism is determined, modulo signs, by this fact). Via this isomorphism, one can identify the degree two unramified covering ν_α with a degree two isogeny $\widetilde{\nu} : E' \to E$.

Recall that E can be written by the Weierstrass equation $y^2 = x^3 + 5Dx^2 + 4D^2x$, and that the degree two isogenies are determined by a non-trivial 2-torsion point.

By Lemma 22, we have $\psi_P(\tau_0\tau_3(P)) = \epsilon(0) = (0,0)$. But $\tau_0\tau_3(P)$ also belongs to $\nu_\alpha(F'_\alpha(K))$, and hence $(0,0)$ must be in $\widetilde{\nu}(E'(\mathbb{Q}))$, thus determining the isogeny as the one corresponding to $(0,0)$.

Now we use the standard descent via a 2-isogeny. One gets that $E(\mathbb{Q})/\widetilde{\nu}(E'(\mathbb{Q}))$ is injected inside the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by -1 and the prime divisors of $4D^2$. Since D is prime, the only possibilities are -1, 2 and D, which become only -1 and D over $K^*/(K^*)^2$. Hence, we need only four twists of $\widetilde{\nu}$ over K in order to cover all the points of $E(\mathbb{Q})$. Note that the twist corresponding to 1 is identified with ν_α. To find the twist corresponding to -1 one can argue in the following way: when changing the field K to $K(\sqrt{-1})$ then -1 becomes equal 1 modulo squares and not D or $-D$, and the same applies to α and $-\alpha$. Hence -1 is identified to $\nu_{-\alpha}$. A similar argument, but using that $\alpha\overline{\alpha}$ is equal to D modulo squares in K, shows that D corresponds to $\nu_{\overline{\alpha}}$. □

In order to obtain from these coverings of $F_D^{(4)}$ some coverings of C_D we write C_D in a different form, the one given by the following equations in $\mathbb{A}^3$:

$$C_D : \{ \, DX_3^2 = q(t) \, , \, X_4^2 = p(t) \, \}$$

where $p(t) := t^4 - 12t^3 + 2t^2 + 12t + 1$. Then the above lemma implies that any rational point of C_D, modulo the automorphisms in Υ, comes from a point in K of one of the curves C'_δ, with $\delta = \alpha$ or $\delta = -\alpha$, given by the following equations in $\mathbb{A}^4$:

$$C'_\delta : \{ \, \delta y_1^2 = q_1(t) \, , \, (D/\delta) y_2^2 = q_2(t) \, , \, X_4^2 = p(t) \, \}$$

(and, moreover, with $t \in \mathbb{Q}$) by the natural map μ_δ. Observe, before continuing, that any rational point in C_D comes from a point in the affine part in the form above, which is singular at infinity, since D is not a square in $\mathbb{Q}$.

Now we consider the following hyperelliptic quotient H_δ of the curve C'_δ, which can be described by the equation

$$H_\delta \, : \, \delta W^2 = q_1(t)p(t),$$

and where the quotient map η is determined by saying that $W = y_1X_4$.

The following lemma is an easy verification.

Lemma 24. *Let E_δ be the elliptic curve defined by the equation*

$$E_\delta \, : \, \delta y^2 = x^3 + 5\sqrt{2}x^2 - x.$$

Then there exists a non-constant morphism from the genus 2 curve H_δ to E_δ:

$$\varphi : H_\delta \to E_\delta \, , \quad \varphi(t,W) = \left(\frac{-2(-3+2\sqrt{2})q_1(t)}{(t-\sqrt{2}+1)^2}, \frac{3(-4+3\sqrt{2})W}{(t-\sqrt{2}+1)^3} \right).$$

Remark 25. The group of automorphism of the genus 2 curve H_δ is generated by a non-hyperelliptic involution τ and by the hyperelliptic involution ω. Then we have that the elliptic curve E_δ is $H_\delta/\langle\tau\rangle$. The other elliptic quotient E'_δ is obtained by $\tau\omega$, that is $E'_\delta = H_\delta/\langle\tau\omega\rangle$. It is easy to compute that $E'_\delta \, : \, \delta y^2 = x^3 + 9\sqrt{2}x^2 - 81x$. Therefore, $\mathrm{Jac}(H_\delta)$ is $\mathbb{Q}(\sqrt{2})$-isogenous to $E_\delta \times E'_\delta$. Moreover, E_1 and E'_1 are $\mathbb{Q}(\sqrt{2})$-isomorphic respectively to `384F2` and `384C2` in Cremona's tables, so E_δ and E'_δ are δ-twists of them.

Remark 26. The fact that H_δ has such elliptic quotient defined over K is the main reason we consider this specific 2-coverings of C_D. If we want to do the same arguments with other 2-coverings, coming from 2-coverings of $F_D^{(4)}$ or from 2-coverings of other genus 1 quotients $F_D^{(i)}$, we will not get such a quotient defined over a quadratic extension of $\mathbb{Q}$.

In the following proposition we will determine a finite subset of $E_\delta(K)$ containing the image of the points Q in $C_\delta(K)$ such that $\mu_\delta(Q) \in C_D(\mathbb{Q})$.

Proposition 27. *Let D be a squarefree integer with $D \equiv 1 \pmod{24}$. Consider $P \in C_D(\mathbb{Q})$. Then there exists $\tau \in \Upsilon$ such that $\tau(P) = \mu_\delta(Q)$ for $\delta = \alpha$ or $\delta = -\alpha$, with $Q \in C'_\delta(K)$. Let $R := \varphi(\eta(Q)) \in E_\delta(K)$ be the corresponding point in E_δ. Then*

$$R \in \{(x,y) \in E_\delta(K) \mid \pi(x,y) := \frac{2(-4+2\sqrt{2}-x(1-\sqrt{2}))}{(6-4\sqrt{2}-x)} \in \mathbb{Q}\}.$$

Proof. Part of the lemma is a recollection of what we have proved in lemmas above. Only the last assertion needs a proof. So, suppose we have a point $Q \in C'_\delta(K)$ such that $\mu_\delta(Q) \in C_D(\mathbb{Q})$. Then the t-coordinate of Q is in $\mathbb{Q}$, since μ_δ leaves the t-coordinate unchanged. This implies that the x-coordinate of $R := \varphi(\eta(Q))$, that is $\frac{-2(-3+2\sqrt{2})q_1(t)}{(-1+\sqrt{2}-t)^2}$, must come from a rational number t. This again implies that the sum of the t-coordinates of the two pre-images of R is a rational number. But this sum can be expressed in the x-coordinate of R as $\pi(x,y)$. $\square$

The following diagram illustrates all the curves and morphisms involved in our problem:

$$\begin{tikzcd}
 & C'_\delta \arrow[dl, "\mu_\delta"'] \arrow[dd] \arrow[dr, "\eta"] & & \\
C_D \arrow[d, "\phi^{(4)}"'] & & H_\delta \arrow[d, "\varphi"] & \\
F_D^{(4)} & F'_\delta \arrow[l, "\nu_\delta"'] & E_\delta \arrow[r, "\pi"] & \mathbb{P}^1
\end{tikzcd}$$

Hence, to find all the points in $C_D(\mathbb{Q})$ is sufficient to find all the points (x,y) in $E_\delta(K)$ such that $\pi(x,y) \in \mathbb{Q}$ for $\delta = \alpha$ or $\delta = -\alpha$. But this is what the so-called elliptic Chabauty does, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1. And this seems to be our case in the cases we consider.

Example 28. We consider the case $D = 409$. The 16 points $[\pm 7, \pm 13, \pm 17, 1, \pm 23]$ give the 8 points in $F_{409}^{(4)}$ with $t \in \{-3/2, -5, 2/3, 1/5\}$. Take $\alpha := 21 + 4\sqrt{2}$, which satisfies the hypothesis of Lemma 23. Then the 8 points in C_{409} with $t = -3/2$ and $t = -5$ come from the 16 points in C'_α given by $[t, y_1, y_2, X_4] = [-3/2, \pm 1/2, \pm 1/2, \pm 23/4]$ and $[-5, \pm\sqrt{2}, \pm\sqrt{2}, \pm 46]$ respectively, which in turn give the 4 points in H_α given by $[t, W] = [-3/2, \pm 23/8]$ and $[-5, \pm 46\sqrt{2}]$. Finally, this 4 points gives the following 2 points R and $-R$ in E_α:

$$\left(\frac{-2}{49}(-663+458\sqrt{2}), \pm\frac{69}{343}(-232+163\sqrt{2})\right).$$

The other points with $t = 2/3$ and $1/5$ rise to points in $E_{-\overline{\alpha}}(K)$, as shown in Lemma 23. We will show that these points in $E_\alpha(K)$ are the only points R with $\pi(R) \in \mathbb{Q}$, and that there are no such points in $E_{-\alpha}(K)$.

Elliptic Chabauty. In order to apply the elliptic Chabauty technique, we need first to fix a rational prime p such that it is inert over K and E_δ has good reduction over such p. The smallest such prime under our conditions is $p = 5$, since $D \equiv \pm 1 \pmod 5$. Denote by $\widetilde{E_\delta}$ the reduction modulo 5 of E_δ, which is an elliptic curve over $\mathbb{F}_{25} := \mathbb{F}_5(\sqrt{2})$. Then the elliptic Chabauty method will allow us to bound, for each point $\widetilde{R}$ in $\widetilde{E_\delta}(\mathbb{F}_{25})$, the number of points R in $E_\delta(K)$ reducing to that point $\widetilde{R}$ and such that $\pi(R) \in \mathbb{Q}$, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1. In the next lemma we will show that in fact we only need to consider fourth (or two) points in $\widetilde{E_\delta}(\mathbb{F}_{25})$, instead of all the 32 points.

Lemma 29. *Let D be a squarefree integer such that $D \equiv \pm 1 \pmod 5$, and let $\delta \in \mathbb{Z}[\sqrt{2}]$ and $Q \in C'_\delta(K)$ be such that $\mu_\delta(Q) \in C_D(\mathbb{Q})$. Let $R := \varphi(\eta(Q)) \in E_\delta(K)$ be the corresponding point in E_δ. Then $\pi(R) \equiv -1 \pmod 5$ or $\pi(R) \equiv \infty \pmod 5$.*

Moreover, if the rank of the group of points $E_\delta(K)$ is equal to 1, the torsion subgroup has order 2, and the reduction of the generator has order 4, then only one of the two cases can occur.

Proof. We repeat the whole construction of the coverings, but modulo 5. First, observe that, since $D \equiv \pm 1 \pmod 5$, the only $\mathbb{F}_5$-rational points of $\widetilde{C_D}$ are the ones with coordinates $[\pm 1 : \pm 1 : \pm 1 : 1 : \pm 1]$. So the t-coordinates of this points are $t = 0, 1, 4$ and ∞. Substituting this values in $q_1(t)$ modulo 5, we always get squares in $\mathbb{F}_{25}$. This implies that all the twists of the curves involved are all isomorphic modulo 5 to the curves with $\delta = 1$.

Consider the curve $\widetilde{H_1}$ over $\mathbb{F}_{25}$. An easy computation shows that the only points in $\widetilde{H_1}$ whose t-coordinate is rational are the points with $t = 0$, $t = 1$ and the two points at infinity. Now, this points have image by φ in $\widetilde{E_1}$ equal to the points with x-coordinate equal to $-\overline{\xi} = -1 + \sqrt{2}$ in the first two cases, and equal to $\xi = 1 + \sqrt{2}$ for the points at infinity. In the first case we have that $\pi(-1 + \sqrt{2}) \equiv -1 \pmod 5$, and in the second one we have $\pi(1 + \sqrt{2}) \equiv \infty \pmod 5$.

Now, the curve $\widetilde{E_1}$, given by the equation $y^2 = x^3 + 4x$, has 32 rational points over $\mathbb{F}_{25}$, and $\widetilde{E_1}(\mathbb{F}_{25}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ as abelian group, with generators some points P_4 and P_8 with x-coordinate equal to $\xi = 1 + \sqrt{2}$ and $\sqrt{2}\xi = 2 + \sqrt{2}$ respectively. We have then that

$$\{R \in \widetilde{E_1}(\mathbb{F}_{25}) \mid \pi(R) = \infty\} = \{P_4, -P_4\}$$

and

$$\{R \in \widetilde{E_1}(\mathbb{F}_{25}) \mid \pi(R) = -1\} = \{2P_8 + P_4, -2P_8 - P_4\}.$$

Now, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1, the torsion subgroup has order 2, and the reduction of the generator has order 4, then the reduction of $E_\delta(K)$ is a subgroup of $\widetilde{E_1}(\mathbb{F}_{25})$ isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But the subgroup generated by P_4 and $2P_8 + P_4$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, hence the reduction cannot contain both points. $\square$

In order to use elliptic Chabauty, it is convenient to transform the equation that gives E_δ into a Weierstrass equation, by doing the standard transformation sending (x, y) to $(\delta x, \delta y)$. We get the equation

$$y^2 = x^3 + 5\sqrt{2}\delta x^2 - \delta^2 x.$$

We will denote by abuse of notation this elliptic curve by E_δ. Moreover, the map π becomes the map $f : E_\delta \to \mathbb{P}^1$, given by

$$f(x) := \frac{(2\sqrt{2}-2)x + \delta(4\sqrt{2}-8)}{\delta(-4\sqrt{2}+6) - x}.$$

Let us explain first the idea of the elliptic Chabauty method. For a given D, we fix a $\delta = \alpha$ or $\delta = -\alpha$, and we want to compute the set

$$\Omega_\delta := \{Q \in E_\delta(K) \mid f(Q) \in \mathbb{Q} \text{ and } f(Q) \equiv -1, \infty \pmod 5\}.$$

As we already remarked, we need first to compute the rank of the group $E_\delta(K)$, which should be less or equal to one. We will also need to know explicitly the torsion subgroup of that group, and some non-torsion point if the rank is 1, which is not an ℓ-multiple of a K-rational point for some primes ℓ to be determined (in our cases they will be only $\ell = 2$). In the cases we already know some points in $E_\delta(K)$, those coming from the known points in $C_D(\mathbb{Q})$, we will show that those points are non-torsion points.

We have two cases we want to consider. The first case is when we will not know any point $R \in E_\delta(K)$ such that $f(R) \in \mathbb{Q}$. In these cases we hope to show that $\Omega_\delta = \emptyset$ by just proving that the reduction of the group $E_\delta(K)$ does not contain any point $\widetilde{Q}$ such that $\widetilde{f}(\widetilde{Q}) \in \mathbb{F}_5$. We do so for the two cases in the following lemma.

Lemma 30. *Take $D = 409$ and $\alpha = 21 + 4\sqrt{2}$. Then the elliptic curves E_α and $E_{-\alpha}$ have rank 1 over K. All of them have torsion part isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and generated by the point $(0,0)$. The points $P = ((-30\sqrt{2} - 43)/2, (759\sqrt{2} + 1104)/4)$ in $E_\alpha(K)$ and the point $P' \in E_{-\alpha}(K)$ with x-coordinate equal to*

$$\frac{29769295809708\sqrt{2} + 42339835565318}{4185701809}$$

are non torsion points and not 2-divisible in K.

Moreover, all the points R in the set $\Omega_{-\alpha}$ verify that $f(R) \equiv \infty \pmod 5$, and all the points R in the set Ω_α verify that $f(R) \equiv -1 \pmod 5$.

Proof. The bounds for the rank of the group $E_\delta(K)$ are obtained by using the Denis Simon's `GP/PARI` scripts as contained in `SAGE`, or the RankBound function in `MAGMA`. The points P and P' are obtained by search (using one of the programs mention before), and one gets also by 2-descent that they are not 2-divisible. Observe also that $R + (0,0) = P$, where R is the point computed in the example 28 so we could take R instead of P.

The last assertions are shown by proving that the subgroup generated by the reduction modulo 5 of the point P' and the point $(0,0)$ does not contain any point with image by $\widetilde{f}$ equal to -1, and that the subgroup generated by the reduction modulo 5 of the point P and the point $(0,0)$ does not contain any point with image by $\widetilde{f}$ equal to ∞. These last two cases are in fact instances of the previous lemma, since the reduction of the points P and P' have order 4. $\square$

Now, in order to show that $\Omega_{-\alpha}$ is in fact empty, we need to use information on some other primes. That is what we do in the following lemma.

Lemma 31. *Take $D = 409$ and $\alpha = 21 + 4\sqrt{2}$. Then $\Omega_{-\alpha} = \emptyset$.*

Proof. By using reduction modulo 5, we get that any point R in $\Omega_{-\alpha}$ should be of the form $R = (4n+1)P' + (0,0)$ for some $n \in \mathbb{Z}$, since it should reduce to the point $\widetilde{P' + T}$, and the order of $\widetilde{P'}$ is 4.

Now we reduce modulo 13. One shows easily that the order of P' modulo 13 is equal to 24, and that the points $R \in E_{-\alpha}(K)$ such that $f(R) \in \mathbb{P}^1(\mathbb{Q})$ reduce to the points $6P'$ or $12P' + (0,0)$. Hence the points R should be of the form $R = (24n+6)P'$ or $(24n+12)P' + (0,0)$. Comparing with the result obtained from the reduction modulo 5, we get that there is no such point. □

The second case in when we already know some points $R \in \Omega_\delta$. Then our objective will be to show there are no more, by showing that the set

$$\Omega_{\delta,R} := \{Q \in E_\delta(K) \mid Q \in \Omega_\delta \text{ and } Q \equiv R \pmod 5\}$$

only contains the point R. This is done by translating the problem of computing the number of points in $\Omega_{\delta,R}$ into a problem of computing the number of p-adic zeros of some formal power series, and using Strassmann's Theorem to do so.

Proposition 32. *Take $\alpha = 21 + 4\sqrt{2}$, and consider the point*

$$R = \left(\frac{-2}{49}(-663 + 458\sqrt{2}), \frac{69}{343}(-232 + 163\sqrt{2}) \right).$$

Then

$$\Omega_\alpha = \{Q \in E_\alpha(K) \mid f(Q) \in \mathbb{Q} \text{ and } f(Q) \equiv -1 \pmod 5\} = \{R, -R\}.$$

Proof. First of all, observe that the order of the reduction of P modulo 5 is 4. Also, any point R' in Ω_α reduces modulo 5 to the points $\pm R$, so it is of the form $\pm R + 4nP$. We are going to prove there is only one point in Ω_α reducing to R, and we deduce the other case by using the -1-involution.

Observe that any point in $E_\alpha(K)$ that reduces to 0 modulo 5 is of the form $4nP$ for some $n \in \mathbb{Z}$. We are going to compute the z-coordinate of that points, where $z = -x/y$ if $P = (x, y)$, as a formal power series in n. Denote by z_0 the z-coordinate of $4P$. The idea is to use the formal logarithm $\log_E$ and the formal exponential $\exp_E$ of the formal group law associated to E_α. These are formal power series in z, one inverse to the other with respect to the composition, and such that

$$\log_E(z\text{-coord}(G + G')) = \log_E(z\text{-coord}(G)) + \log_E(z\text{-coord}(G'))$$

for any G and G' reducing to 0 modulo 5, and where the power series are evaluated in the completion of K at 5. Thus, we get that

$$z\text{-coord}(n(4P)) = \exp_E(n \log_E(z_0)),$$

which is a power series in n.

Now, we are going to compute $f(R+4nP)$ as a power series in n. To do so we use that, by the addition formulae,

$$x\text{-coord}(R+G) = \frac{w(z)(1+y_0w(z))^2 - (a_2w(z)+z+x_0w(z))(z-x_0w(z))^2}{w(z)(z-x_0w(z))^2}$$

where $R=(x_0,y_0)$, $a_2 = 5\sqrt{2}\alpha$, z is the z-coordinate of a point G reducing to 0 modulo 5 and $w(z) = -1/y$ evaluated as a power series in z. This function is a power series in z, starting as $x\text{-coord}(R+G) = x_0 + 2y_0z + (3x_0^2 + 2a_2x_0 + a_4)z^2 + O(z^3)$, where $a_4 = -\alpha^2 = y^2/x - (x^2 + 5\sqrt{2}\alpha x)$. Hence we get that $f(R+4nP) = f(x\text{-coord}(R+n(4P))$ can be expressed as a power series $\Theta(n)$ in n with coefficients in K. We express this power series as $\Theta(n) = \Theta_0(n) + \sqrt{2}\Theta_1(n)$, with $\Theta_i(n)$ now being a power series in $\mathbb{Q}$. Then $f(R+4nP)\in\mathbb{Q}$ for some $n\in\mathbb{Z}$ if and only if $\Theta_2(n)=0$ for that n. Observe also that, since $f(R)\in\mathbb{Q}$, we will get that $\Theta_2(0)=0$, so $\Theta_2(n) = j_1n + j_2n^2 + j_3n^3 + \cdots$. To conclude, we will use Strassmann's Theorem: if the 5-adic valuation of j_1 is strictly smaller that the 5-adic valuation of j_i for any $i>1$, then this power series has only one zero at $\mathbb{Z}_5$, and this zero is $n=0$. In fact, one can easily shown that this power series verifies that the 5-adic valuation of j_i is always greater or equal to i, so, if we show that $j_1 \not\equiv 0 \pmod{5^2}$ we are done.

In order to do all this explicitly, we will work modulo some power of 5. In fact, working modulo 5^2 will be sufficient. We have that $z_0 = z\text{-coord}(4P) \equiv -10\sqrt{2}+5 \pmod{5^2}$, and that $z\text{-coord}(n(4P)) \equiv (15\sqrt{2}+5)n \pmod{5^2}$. Finally, we get that $\Theta(n) \equiv 19 + (15\sqrt{2} + 20)n \pmod{5^2}$, hence $\Theta_2(n) \equiv 15n \pmod{5^2}$, so $j_1 \equiv 15 \pmod{5^2}$ and we are done. □

An alternative way of proving this result is to use the build-in `MAGMA` function `Chabauty` at the prime 5, together with the auxiliary prime 13 (which will help to discard some cases with a Mordell-Weil sieve argument). The answer is that there are only 2 points R' in $E_\alpha(K)$ such that $f(R')\in\mathbb{Q}$, both having $f(R') = 13/2$. Since we already have two points $\pm R$, both giving $f(R) = 13/2$, we are done.

8. Explicit computations and conjectures

We have followed two different approaches to compute for which squarefree integers D there are non-constant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{D})$. On one hand, for each D we have checked if D passes all the sieves from the previous sections, obtaining the following result.

Corollary 33. *Let $D < 10^{13}$ be a squarefree integer such that $C_D(\mathbb{Q}) \neq \emptyset$, then $D = 409$ or $D = 4688329$.*

Proof. First, for each D we have passed all the local conditions (Proposition 6) and the conditions coming from the Mordell-Weil sieve (Corollary 21). Only 1048 values of D have passed these sieves. To discard all the values except $D = 409$ and $D = 4688329$, we first apply a test derived from Proposition 18. We test if, for any prime q dividing such D, there is an odd multiple kP of the point $P := (6, 24) \in E^{(1)}(\mathbb{Q})$ reducing to a point with x-coordinate equal to -18 modulo q. To verify explicitly this condition, we compute first if there is a point Q in $E^{(1)}(\mathbb{F}_q)$, the order O_q of P in $E^{(1)}(\mathbb{F}_q)$ and the discrete logarithm $\log(Q, P)$, i.e. the number k such that $Q = kP$, if it exists. In case there is no such Q

or there is no such logarithm, then D does not pass the test. Also in case k and O_q are even. In case it passes this first test, we combine this information with the information from the computation of the $M_D^{(q)}$ for the first 100 primes to discard some other cases.

After this last test there are 34 values of D that survive, and we pass then a test based on the ternary forms criterium given by Proposition 15, by using a short program in SAGE done by Gonzalo Tornaria. We check that for these values $r(D, 3x^2+9y^2+16z^2) \neq r(D, x^2+3y^2+144z^2)$. Hence for those values of D, $L(E_D^{(2)}, 1) \neq 0$, so the analytic rank of $E_D^{(2)}$ is zero, hence their rank is also 0.

Only $D = 409$ and $D = 4688329$ survive all these tests, but for these values we do have points in $C_D(\mathbb{Q})$. □

On the other hand, we have an isomorphism $\psi : E^{(1)} \longrightarrow F^{(3)}$ defined by

$$\psi(P) = \left(\frac{6-x}{6+3x-y}, \frac{-72-108x-18x^2+x^3+48y}{(6+3x-y)^2} \right),$$

if $P = (x, y) \neq (-2, 0), (-3, -3), (6, 24)$ and $\psi(6, 24) = \left(\frac{2}{3}, \frac{23}{9}\right)$, $\psi(-2, 0) = \infty_1$ and $\psi(-3, -3) = \infty_2$, where ∞_1 and ∞_2 denote the two branches at infinity at the desingularization of $F^{(3)}$ at the unique singular point $[0 : 1 : 0] \in \mathbb{P}^2$. This construction allows us to construct all the non-constant arithmetic progressions of five squares over all quadratic fields. Let $P = (2, -8)$, a generator of the free part of $E^{(1)}(\mathbb{Q})$, and let n be a positive integer. Let $(t_n, z_n) = \psi([n]P)$. Now, consider the next squarefree factorization of the number

$$t_n^4 - 8t_n^3 + 2t_n^2 + 8t_n + 1 = D_n w_n^2,$$

where $D_n \in \mathbb{Z}$ is squarefree, $w_n \in \mathbb{Q}$. Therefore the following sequence defines a non-contant arithmetic progression of 5 squares over $\mathbb{Q}(\sqrt{D_n})$:

$$(-t_n^2 - 2t_n + 1)^2 \ , \ (t_n^2 + 1)^2 \ , \ (t_n^2 - 2t_n - 1)^2 \ , \ D_n \, w_n^2 \ , \ z_n^2 \, ,$$

and we have points $Q_n := [-t_n^2 - 2t_n + 1 \, : \, t_n^2 + 1 \, : \, t_n^2 - 2t_n - 1 \, : \, w_n \, : \, z_n] \in C_{D_n}(\mathbb{Q})$.

Remark 34. Observe that the pairs (D_n, Q_n) constructed in this way are distinct for distinct n. On the other hand, we cannot be sure that all the fields $\mathbb{Q}(\sqrt{D_n})$ are distinct. However, we do have an infinite number of integers D such that $C_D(\mathbb{Q}) \neq \emptyset$. This is because for any integer D, the curve C_D, being of genus 5 (greater than 1), has always a finite number of rational points. Since we do have an infinite number of pairs (D_n, Q_n) with $Q_n \in C_{D_n}(\mathbb{Q})$, we do have and infinite number of distinct D_n.

Remark 35. If we replace P by $Q \in \{[n_1]T_1 + [n_2]T_2 + [m]P_0 \,|\, n_1, n_2 \in \{0, 1\}, \, m \in \{n, -n-1\}\}$, where $T_1 = (-2, 0)$ and $T_2 = (-6, 0)$ is a basis of $E^{(1)}(\mathbb{Q})_{\text{tors}}$, we obtain the same arithmetic progression (up to equivalence). Note that if $n = 0$, then we obtain $D_0 = 1$ and the above sequence is the constant arithmetic progression.

We summarize in the following tables the computations that we have made using the above algorithm. We have normalized the elements of the arithmetic progressions to obtain integers and without squares in common. We have splitted in two tables. In the first one appears n and the factorization of D_n. In the second table appear for each value of n the corresponding factorization of X_0. For all the values of n computed,

we have obtained that the fourth element of the arithmetic progression is $\sqrt{D_n}$ (in the notation above, $w_n = 1$). That is, if we denote by $r = (D_n - X_0^2)/3$, then the sequence $\{X_k^2 = X_0^2 + k\,r \mid k \in \{0, \dots, 4\}\}$ defines an arithmetic progression over $\mathbb{Q}(\sqrt{D_n})$.

n	D_n
1	409
2	4688329
3	$457 \cdot 548240447113$
4	19955489409130366807320 1
5	$4343602906873 \cdot 5331395003998418925451 3$
6	$2593 \cdot 9697 \cdot 4100179090153 \cdot 29331869174167888116692693659 3$
7	33082351395282824357312248053607753315606400013911972464229586192 1
8	$24697 \cdot 303049 \cdot 921429638596379458921 \cdot 291824110407387399760153 \cdot 346275704903307113776829188636 9$

n	X_0
1	7
2	$47 \cdot 89$
3	$31 \cdot 113 \cdot 577$
4	$7 \cdot 176201 \cdot 515087$
5	$2111 \cdot 133967 \cdot 1134755801$
6	$119183 \cdot 12622601 \cdot 2189366343649$
7	$2^{10} \cdot 3 \cdot 17 \cdot 73 \cdot 103787 \cdot 112261 \cdot 963877 \cdot 20581582583$
8	$2^{38} \cdot 3^2 \cdot 5 \cdot 7 \cdot 23 \cdot 102179447 \cdot 1017098920090613939$

An arithmetic progression of five squares over $\mathbb{Q}(\sqrt{D_n})$

One can observe that the size of the D_n we encounters grow very fast, but we do not know if the D_n constructed in this way always verify that $D_n < D_{n+1}$. We guess that this condition holds. Even more, the above table and the Corollary 33 suggest that, in fact, there does not exist any squarefree integer D such that $C_D(\mathbb{Q}) \neq \emptyset$ and $D_n < D < D_{n+1}$.

If we only use the results in section 4 (Proposition 6) and section 6 (Corollary 21), we get that the number of squarefree integers D that pass both tests have positive (but small) density. This is possibly true if we use also the condition of the rank, for example Proposition 15, since the number of twists with positive rank of a fixed elliptic curve should have also positive density. But we suspect that the number of actual square-free integers D such that C_D has rational points should have zero density.

Data: All the `MAGMA` and `SAGE` sources are available from the first author webpage.

References

[1] E. Bombieri, A. Granville and J. Pintz, Squares in arithmetic progressions. Duke Math. J. 66 (1992), no. 3, 369–385.

[2] E. Bombieri and U. Zannier, A note on squares in arithmetic progressions. II. Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl. 13 (2002), no. 2, 69–75.

[3] N. Bruin, Chabauty methods using elliptic curves. J. Reine Angew. Math. 562 (2003), 27 - 49.

[4] N. Bruin and E. V. Flynn, Towers of 2-covers of hyperelliptic curves, Trans. Amer. Math. Soc. 357 (2005), 4329-4347.

[5] J.J. Cannon, W. Bosma (Eds.), Handbook of Magma Functions. Edition 2.15-6 (2009).

[6] K.R. Coombes and D. Grant, On heterogeneos spaces, Journal of the London Mathematical Society, series 2, 40 (3) (1989),385-397

[7] J. E. Cremona, Algorithms for modular elliptic curves. Cambridge University Press 1992.

[8] E.V. Flynn and J.L. Wetherell, Covering collections and a Challenge Problem of Serre, Acta Arith. 98 (2001), 197-205

[9] E. González-Jiménez and J. Steuding, Arithmetic progressions of four squares over quadratic fields. arXiv: 0903.3856.

[10] D. E. Rohrlich, Galois theory, elliptic curves, and root numbers, Comp. Math. 100 (1996), no. 3, 311-349.

[11] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986.

[12] W. Stein et al., Sage: Open Source Mathematical Software (Version 4.0), The Sage Group, 2009, http://www.sagemath.org.

[13] X. Xarles, Squares in arithmetic progression over number fields. arXiv: 0909.1642.

[14] S. Yoshida, Some variants of the congruent number problem II. Kyushu J. Math. 56 (2002), 147–165.

[15] J.L. Wetherell, Bounding the Number of Rational Points on Certain Curves of High Rank, PhD Dissertation (1997), University of California at Berkeley.

Universidad Autónoma de Madrid, Departamento de Matemáticas and Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM), Madrid, Spain

E-mail address: enrique.gonzalez.jimenez@uam.es

Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain

E-mail address: xarles@mat.uab.cat